Nhanhq_Scanner

Report generated by Nessus™ Tue, 08 Sep 2020 13:37:12 EDT

TABLE OF CONTENTS

Vulnerabilities by Host

Vulnerabilities by Host

192.168.230.130

CRITICAL	HIGH	MEDIUM	LOW	INFO
1	1	1	0	39

Scan Information

Start time: Tue Sep 8 13:25:10 2020
End time: Tue Sep 8 13:37:12 2020

Host Information

Netbios Name: WIN-IEJFU67798L
IP: 192.168.230.130
MAC Address: 00:0C:29:D9:0D:13
OS: Microsoft Windows 7 Enterprise

Vulnerabilities

108797 - Unsupported Windows OS (remote)

Synopsis

The remote OS or service pack is no longer supported.

Description

The remote version of Microsoft Windows is either missing a service pack or is no longer supported. As a result, it is likely to contain security vulnerabilities.

See Also

https://support.microsoft.com/en-us/lifecycle

Solution

Upgrade to a supported service pack or operating system

Risk Factor

Critical

CVSS v3.0 Base Score

9.8 (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H)

CVSS Base Score

10.0 (CVSS2#AV:N/AC:L/Au:N/C:C/I:C/A:C)

References

XREF IAVA:0001-A-501

Plugin Information

Published: 2018/04/03, Modified: 2020/08/25

Plugin Output

tcp/0

```
The following Windows version is installed and not supported:

Microsoft Windows 7 Enterprise
```

97833 - MS17-010: Security Update for Microsoft Windows SMB Server (4013389) (ETERNALBLUE) (ETERNALCHAMPION) (ETERNALROMANCE) (ETERNALSYNERGY) (WannaCry) (EternalRocks) (Petya) (uncredentialed check)

Synopsis

The remote Windows host is affected by multiple vulnerabilities.

Description

The remote Windows host is affected by the following vulnerabilities :

- Multiple remote code execution vulnerabilities exist in Microsoft Server Message Block 1.0 (SMBv1) due to improper handling of certain requests. An unauthenticated, remote attacker can exploit these vulnerabilities, via a specially crafted packet, to execute arbitrary code. (CVE-2017-0143, CVE-2017-0144, CVE-2017-0145, CVE-2017-0146, CVE-2017-0148)

- An information disclosure vulnerability exists in Microsoft Server Message Block 1.0 (SMBv1) due to improper handling of certain requests. An unauthenticated, remote attacker can exploit this, via a specially crafted packet, to disclose sensitive information. (CVE-2017-0147)

ETERNALBLUE, ETERNALCHAMPION, ETERNALROMANCE, and ETERNALSYNERGY are four of multiple Equation Group vulnerabilities and exploits disclosed on 2017/04/14 by a group known as the Shadow Brokers. WannaCry / WannaCrypt is a ransomware program utilizing the ETERNALBLUE exploit, and EternalRocks is a worm that utilizes seven Equation Group vulnerabilities. Petya is a ransomware program that first utilizes CVE-2017-0199, a vulnerability in Microsoft Office, and then spreads via ETERNALBLUE.

See Also

http://www.nessus.org/u?68fc8eff

http://www.nessus.org/u?321523eb

http://www.nessus.org/u?065561d0

http://www.nessus.org/u?d9f569cf

https://blogs.technet.microsoft.com/filecab/2016/09/16/stop-using-smb1/

http://www.nessus.org/u?b9d9ebf9

http://www.nessus.org/u?8dcab5e4

http://www.nessus.org/u?234f8ef8

http://www.nessus.org/u?4c7e0cf3

https://github.com/stamparm/EternalRocks/

http://www.nessus.org/u?59db5b5b

Solution

Microsoft has released a set of patches for Windows Vista, 2008, 7, 2008 R2, 2012, 8.1, RT 8.1, 2012 R2, 10, and 2016. Microsoft has also released emergency patches for Windows operating systems that are no longer supported, including Windows XP, 2003, and 8.

For unsupported Windows operating systems, e.g. Windows XP, Microsoft recommends that users discontinue the use of SMBv1. SMBv1 lacks security features that were included in later SMB versions. SMBv1 can

be disabled by following the vendor instructions provided in Microsoft KB2696547. Additionally, US-CERT recommends that users block SMB directly by blocking TCP port 445 on all network boundary devices. For SMB over the NetBIOS API, block TCP ports 137 / 139 and UDP ports 137 / 138 on all network boundary devices.

Risk Factor

High

CVSS v3.0 Base Score

8.1 (CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H)

CVSS v3.0 Temporal Score

7.7 (CVSS:3.0/E:H/RL:O/RC:C)

CVSS Base Score

9.3 (CVSS2#AV:N/AC:M/Au:N/C:C/I:C/A:C)

CVSS Temporal Score

8.1 (CVSS2#E:H/RL:OF/RC:C)

STIG Severity

I

References

BID	96703
BID	96704
BID	96705
BID	96706
BID	96707
BID	96709
CVE	CVE-2017-0143
CVE	CVE-2017-0144
CVE	CVE-2017-0145
CVE	CVE-2017-0146
CVE	CVE-2017-0147
CVE	CVE-2017-0148
MSKB	4012212
MSKB	4012213
MSKB	4012214
MSKB	4012215
MSKB	4012216

MSKB	4012217
MSKB	4012606
MSKB	4013198
MSKB	4013429
MSKB	4012598
XREF	EDB-ID:41891
XREF	EDB-ID:41987
XREF	MSFT:MS17-010
XREF	IAVA:2017-A-0065

Exploitable With

CANVAS (true) Core Impact (true) Metasploit (true)

Plugin Information

Published: 2017/03/20, Modified: 2019/11/13

Plugin Output

tcp/445/cifs

57608 - SMB Signing not required

Synopsis

Signing is not required on the remote SMB server.

Description

Signing is not required on the remote SMB server. An unauthenticated, remote attacker can exploit this to conduct man-in-the-middle attacks against the SMB server.

See Also

https://support.microsoft.com/en-us/help/887429/overview-of-server-message-block-signing

http://technet.microsoft.com/en-us/library/cc731957.aspx

http://www.nessus.org/u?74b80723

https://www.samba.org/samba/docs/current/man-html/smb.conf.5.html

http://www.nessus.org/u?a3cac4ea

Solution

Enforce message signing in the host's configuration. On Windows, this is found in the policy setting 'Microsoft network server: Digitally sign communications (always)'. On Samba, the setting is called 'server signing'. See the 'see also' links for further details.

Risk Factor

Medium

CVSS v3.0 Base Score

5.3 (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:L/A:N)

CVSS v3.0 Temporal Score

4.6 (CVSS:3.0/E:U/RL:O/RC:C)

CVSS Base Score

5.0 (CVSS2#AV:N/AC:L/Au:N/C:N/I:P/A:N)

CVSS Temporal Score

3.7 (CVSS2#E:U/RL:OF/RC:C)

Plugin Information

Published: 2012/01/19, Modified: 2018/11/15

Plugin Output

tcp/445/cifs

46180 - Additional DNS Hostnames

Synopsis

Nessus has detected potential virtual hosts.

Description

Hostnames different from the current hostname have been collected by miscellaneous plugins. Nessus has generated a list of hostnames that point to the remote host. Note that these are only the alternate hostnames for vhosts discovered on a web server.

Different web servers may be hosted on name-based virtual hosts.

See Also

https://en.wikipedia.org/wiki/Virtual_hosting

Solution

If you want to test them, re-scan using the special vhost syntax, such as :

www.example.com[192.0.32.10]

Risk Factor

None

Plugin Information

Published: 2010/04/29, Modified: 2020/06/12

Plugin Output

tcp/0

```
The following hostnames point to the remote host :
  - win-iejfu67798l
```

45590 - Common Platform Enumeration (CPE)

Synopsis

It was possible to enumerate CPE names that matched on the remote system.

Description

By using information obtained from a Nessus scan, this plugin reports CPE (Common Platform Enumeration) matches for various hardware and software products found on a host.

Note that if an official CPE is not available for the product, this plugin computes the best possible CPE based on the information available from the scan.

See Also

http://cpe.mitre.org/

https://nvd.nist.gov/products/cpe

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2010/04/21, Modified: 2020/08/20

Plugin Output

tcp/0

```
The remote operating system matched the following CPE :

  cpe:/o:microsoft:windows_7:::enterprise
```

10736 - DCE Services Enumeration

Synopsis

A DCE/RPC service is running on the remote host.

Description

By sending a Lookup request to the portmapper (TCP 135 or epmapper PIPE) it was possible to enumerate the Distributed Computing Environment (DCE) services running on the remote port. Using this information it is possible to connect and bind to each service by sending an RPC request to the remote port/pipe.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2001/08/26, Modified: 2020/08/20

Plugin Output

tcp/135/epmap

```
The following DCERPC services are available locally :

Object UUID : 765294ba-60bc-48b8-92e9-89fd77769d91
UUID : d95afe70-a6d5-4259-822e-2c84da1ddb0d, version 1.0
Description : Unknown RPC service
Type : Local RPC service
Named pipe : WindowsShutdown

Object UUID : 765294ba-60bc-48b8-92e9-89fd77769d91
UUID : d95afe70-a6d5-4259-822e-2c84da1ddb0d, version 1.0
Description : Unknown RPC service
Type : Local RPC service
Named pipe : WMsgKRpc0A6080

Object UUID : b08669ee-8cb5-43a5-a017-84fe00000000
UUID : 76f226c3-ec14-4325-8a99-6a46348418af, version 1.0
Description : Unknown RPC service
Type : Local RPC service
Named pipe : WindowsShutdown

Object UUID : b08669ee-8cb5-43a5-a017-84fe00000000
UUID : 76f226c3-ec14-4325-8a99-6a46348418af, version 1.0
Description : Unknown RPC service
Type : Local RPC service
Named pipe : WMsgKRpc0A6080

Object UUID : 6d726574-7273-0076-0000-000000000000
UUID : c9ac6db5-82b7-4e55-ae8a-e464ed7b4277, version 1.0
```

```
Description : Unknown RPC service
Annotation : Impl friendly name
Type : Local RPC service
Named pipe : LRPC-3421f383dd15396daf

Object UUID : 52ef130c-08fd-4388-86b3-6edf00000001
UUID : 12e65dd8-887f-41ef-91bf-8d816c42c2e7, version 1.0
Description : Unknown RPC service
Annotation : Secure Desktop LRPC interface
Type : Local RPC service
Named pipe : WMsgKRpc0A62E1

Object UUID : b08669ee-8cb5-43a5-a017-84fe00000001
UUID : 76f226c3-ec14-4325-8a99-6a46348418af, version 1.0
Description : Unknown RPC service
Type : Local RPC service
Named pipe : WMsgKRpc0A62E1

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 8174bb16-571b-4c38-8386-1102b449044a, version 1.0
Description : Unknown RPC service
Type : Local RPC service
Named pipe : LRPC-b4e9b41d3901dc9528

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : a2d47257-12f7-4beb-8981-0ebfa935c407, version 1.0
Description : Unknown RPC service
Type : Local RPC service
Named pipe : LRPC-b4e9b41d3901dc9528

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 3f31c91e-2545-4b7b-9311-9529e8bffef6, version 1.0
Description : Unk [...]
```

10736 - DCE Services Enumeration

Synopsis

A DCE/RPC service is running on the remote host.

Description

By sending a Lookup request to the portmapper (TCP 135 or epmapper PIPE) it was possible to enumerate the Distributed Computing Environment (DCE) services running on the remote port. Using this information it is possible to connect and bind to each service by sending an RPC request to the remote port/pipe.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2001/08/26, Modified: 2020/08/20

Plugin Output

tcp/445/cifs

```
The following DCERPC services are available remotely :

Object UUID : 765294ba-60bc-48b8-92e9-89fd77769d91
UUID : d95afe70-a6d5-4259-822e-2c84da1ddb0d, version 1.0
Description : Unknown RPC service
Type : Remote RPC service
Named pipe : \PIPE\InitShutdown
Netbios name : \\WIN-IEJFU67798L

Object UUID : b08669ee-8cb5-43a5-a017-84fe00000000
UUID : 76f226c3-ec14-4325-8a99-6a46348418af, version 1.0
Description : Unknown RPC service
Type : Remote RPC service
Named pipe : \PIPE\InitShutdown
Netbios name : \\WIN-IEJFU67798L

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : b58aa02e-2884-4e97-8176-4ee06d794184, version 1.0
Description : Unknown RPC service
Type : Remote RPC service
Named pipe : \pipe\trkwks
Netbios name : \\WIN-IEJFU67798L

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 12345778-1234-abcd-ef00-0123456789ac, version 1.0
Description : Security Account Manager
Windows process : lsass.exe
Type : Remote RPC service
```

```
Named pipe : \pipe\lsass
Netbios name : \\WIN-IEJFU67798L

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 12345778-1234-abcd-ef00-0123456789ac, version 1.0
Description : Security Account Manager
Windows process : lsass.exe
Type : Remote RPC service
Named pipe : \PIPE\protected_storage
Netbios name : \\WIN-IEJFU67798L

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : b25a52bf-e5dd-4f4a-aea6-8ca7272a0e86, version 1.0
Description : Unknown RPC service
Annotation : KeyIso
Type : Remote RPC service
Named pipe : \pipe\lsass
Netbios name : \\WIN-IEJFU67798L

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : b25a52bf-e5dd-4f4a-aea6-8ca7272a0e86, version 1.0
Description : Unknown RPC service
Annotation : KeyIso
Type : Remote RPC service
Named pipe : \PIPE\protected_storage
Netbios name : \\WIN-IEJFU67798L

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 1ff70682-0a51-30e8-076d-740be8cee98b, version 1.0
Description : Scheduler Service
Windows process : svchost.exe
Type : Remote RPC service
Named pipe : \PIPE\atsvc
Netbios name : \\WIN-IEJFU67798L

Obj [...]
```

10736 - DCE Services Enumeration

Synopsis

A DCE/RPC service is running on the remote host.

Description

By sending a Lookup request to the portmapper (TCP 135 or epmapper PIPE) it was possible to enumerate the Distributed Computing Environment (DCE) services running on the remote port. Using this information it is possible to connect and bind to each service by sending an RPC request to the remote port/pipe.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2001/08/26, Modified: 2020/08/20

Plugin Output

tcp/49152/dce-rpc

```
The following DCERPC services are available on TCP port 49152 :

Object UUID : 765294ba-60bc-48b8-92e9-89fd77769d91
UUID : d95afe70-a6d5-4259-822e-2c84da1ddb0d, version 1.0
Description : Unknown RPC service
Type : Remote RPC service
TCP Port : 49152
IP : 192.168.230.130
```

10736 - DCE Services Enumeration

Synopsis

A DCE/RPC service is running on the remote host.

Description

By sending a Lookup request to the portmapper (TCP 135 or epmapper PIPE) it was possible to enumerate the Distributed Computing Environment (DCE) services running on the remote port. Using this information it is possible to connect and bind to each service by sending an RPC request to the remote port/pipe.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2001/08/26, Modified: 2020/08/20

Plugin Output

tcp/49153/dce-rpc

```
The following DCERPC services are available on TCP port 49153 :

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : f6beaff7-1e19-4fbb-9f8f-b89e2018337c, version 1.0
Description : Unknown RPC service
Annotation : Event log TCPIP
Type : Remote RPC service
TCP Port : 49153
IP : 192.168.230.130

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 30adc50c-5cbc-46ce-9a0e-91914789e23c, version 1.0
Description : Unknown RPC service
Annotation : NRP server endpoint
Type : Remote RPC service
TCP Port : 49153
IP : 192.168.230.130

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 3c4728c5-f0ab-448b-bda1-6ce01eb0a6d6, version 1.0
Description : Unknown RPC service
Annotation : DHCPv6 Client LRPC Endpoint
Type : Remote RPC service
TCP Port : 49153
IP : 192.168.230.130

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 3c4728c5-f0ab-448b-bda1-6ce01eb0a6d5, version 1.0
```

```
Description : DHCP Client Service
Windows process : svchost.exe
Annotation : DHCP Client LRPC Endpoint
Type : Remote RPC service
TCP Port : 49153
IP : 192.168.230.130

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 06bba54a-be05-49f9-b0a0-30f790261023, version 1.0
Description : Unknown RPC service
Annotation : Security Center
Type : Remote RPC service
TCP Port : 49153
IP : 192.168.230.130
```

10736 - DCE Services Enumeration

Synopsis

A DCE/RPC service is running on the remote host.

Description

By sending a Lookup request to the portmapper (TCP 135 or epmapper PIPE) it was possible to enumerate the Distributed Computing Environment (DCE) services running on the remote port. Using this information it is possible to connect and bind to each service by sending an RPC request to the remote port/pipe.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2001/08/26, Modified: 2020/08/20

Plugin Output

tcp/49154/dce-rpc

```
The following DCERPC services are available on TCP port 49154 :

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 86d35949-83c9-4044-b424-db363231fd0c, version 1.0
Description : Unknown RPC service
Type : Remote RPC service
TCP Port : 49154
IP : 192.168.230.130

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 552d076a-cb29-4e44-8b6a-d15e59e2c0af, version 1.0
Description : Unknown RPC service
Annotation : IP Transition Configuration endpoint
Type : Remote RPC service
TCP Port : 49154
IP : 192.168.230.130

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 98716d03-89ac-44c7-bb8c-285824e51c4a, version 1.0
Description : Unknown RPC service
Annotation : XactSrv service
Type : Remote RPC service
TCP Port : 49154
IP : 192.168.230.130
```

10736 - DCE Services Enumeration

Synopsis

A DCE/RPC service is running on the remote host.

Description

By sending a Lookup request to the portmapper (TCP 135 or epmapper PIPE) it was possible to enumerate the Distributed Computing Environment (DCE) services running on the remote port. Using this information it is possible to connect and bind to each service by sending an RPC request to the remote port/pipe.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2001/08/26, Modified: 2020/08/20

Plugin Output

tcp/49155/dce-rpc

```
The following DCERPC services are available on TCP port 49155 :

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 12345778-1234-abcd-ef00-0123456789ac, version 1.0
Description : Security Account Manager
Windows process : lsass.exe
Type : Remote RPC service
TCP Port : 49155
IP : 192.168.230.130

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : b25a52bf-e5dd-4f4a-aea6-8ca7272a0e86, version 1.0
Description : Unknown RPC service
Annotation : KeyIso
Type : Remote RPC service
TCP Port : 49155
IP : 192.168.230.130
```

10736 - DCE Services Enumeration

Synopsis

A DCE/RPC service is running on the remote host.

Description

By sending a Lookup request to the portmapper (TCP 135 or epmapper PIPE) it was possible to enumerate the Distributed Computing Environment (DCE) services running on the remote port. Using this information it is possible to connect and bind to each service by sending an RPC request to the remote port/pipe.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2001/08/26, Modified: 2020/08/20

Plugin Output

tcp/49156/dce-rpc

```
The following DCERPC services are available on TCP port 49156 :

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 367abb81-9844-35f1-ad32-98f038001003, version 2.0
Description : Service Control Manager
Windows process : svchost.exe
Type : Remote RPC service
TCP Port : 49156
IP : 192.168.230.130
```

54615 - Device Type

Synopsis

It is possible to guess the remote device type.

Description

Based on the remote operating system, it is possible to determine what the remote system type is (eg: a printer, router, general-purpose computer, etc).

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2011/05/23, Modified: 2011/05/23

Plugin Output

tcp/0

```
Remote device type : general-purpose
Confidence level : 99
```

35716 - Ethernet Card Manufacturer Detection

Synopsis

The manufacturer can be identified from the Ethernet OUI.

Description

Each ethernet MAC address starts with a 24-bit Organizationally Unique Identifier (OUI). These OUIs are registered by IEEE.

See Also

https://standards.ieee.org/faqs/regauth.html

http://www.nessus.org/u?794673b4

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2009/02/19, Modified: 2020/05/13

Plugin Output

tcp/0

```
The following card manufacturers were identified :

00:0C:29:D9:0D:13 : VMware, Inc.
```

86420 - Ethernet MAC Addresses

Synopsis

This plugin gathers MAC addresses from various sources and consolidates them into a list.

Description

This plugin gathers MAC addresses discovered from both remote probing of the host (e.g. SNMP and Netbios) and from running local checks (e.g. ifconfig). It then consolidates the MAC addresses into a single, unique, and uniform list.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2015/10/16, Modified: 2020/05/13

Plugin Output

tcp/0

```
The following is a consolidated list of detected MAC addresses:
  - 00:0C:29:D9:0D:13
```

53513 - Link-Local Multicast Name Resolution (LLMNR) Detection

Synopsis

The remote device supports LLMNR.

Description

The remote device answered to a Link-local Multicast Name Resolution (LLMNR) request. This protocol provides a name lookup service similar to NetBIOS or DNS. It is enabled by default on modern Windows versions.

See Also

http://www.nessus.org/u?51eae65d

http://technet.microsoft.com/en-us/library/bb878128.aspx

Solution

Make sure that use of this software conforms to your organization's acceptable use and security policies.

Risk Factor

None

Plugin Information

Published: 2011/04/21, Modified: 2019/03/06

Plugin Output

udp/5355/llmnr

```
According to LLMNR, the name of the remote host is 'WIN-IEJFU67798L'.
```

117886 - Local Checks Not Enabled (info)

Synopsis

Local checks were not enabled.

Description

Nessus did not enable local checks on the remote host. This does not necessarily indicate a problem with the scan. Credentials may not have been provided, local checks may not be available for the target, the target may not have been identified, or another issue may have occurred that prevented local checks from being enabled. See plugin output for details.

This plugin reports informational findings related to local checks not being enabled. For failure information, see plugin 21745 :

'Authentication Failure - Local Checks Not Run'.

Solution

n/a

Risk Factor

None

References

XREF IAVB:0001-B-515

Plugin Information

Published: 2018/10/02, Modified: 2020/08/25

Plugin Output

tcp/0

```
The following issues were reported :

  - Plugin      : no_local_checks_credentials.nasl
    Plugin ID   : 110723
    Plugin Name : No Credentials Provided
    Message     :
Credentials were not provided for detected SMB service.
```

10394 - Microsoft Windows SMB Log In Possible

Synopsis

It was possible to log into the remote host.

Description

The remote host is running a Microsoft Windows operating system or Samba, a CIFS/SMB server for Unix. It was possible to log into it using one of the following accounts :

- NULL session
- Guest account
- Supplied credentials

See Also

http://www.nessus.org/u?5c2589f6

https://support.microsoft.com/en-us/help/246261

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2000/05/09, Modified: 2020/03/09

Plugin Output

tcp/445/cifs

```
- NULL sessions are enabled on the remote host.
```

10785 - Microsoft Windows SMB NativeLanManager Remote System Information Disclosure

Synopsis

It was possible to obtain information about the remote operating system.

Description

Nessus was able to obtain the remote operating system name and version (Windows and/or Samba) by sending an authentication request to port 139 or 445. Note that this plugin requires SMB1 to be enabled on the host.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2001/10/17, Modified: 2020/01/22

Plugin Output

tcp/445/cifs

```
The remote Operating System is : Windows 7 Enterprise 7601 Service Pack 1
The remote native LAN manager is : Windows 7 Enterprise 6.1
The remote SMB Domain Name is : WIN-IEJFU67798L
```

26917 - Microsoft Windows SMB Registry : Nessus Cannot Access the Windows Registry

Synopsis

Nessus is not able to access the remote Windows Registry.

Description

It was not possible to connect to PIPE\winreg on the remote host.

If you intend to use Nessus to perform registry-based checks, the registry checks will not work because the 'Remote Registry Access'

service (winreg) has been disabled on the remote host or can not be connected to with the supplied credentials.

Solution

n/a

Risk Factor

None

References

XREF IAVB:0001-B-506

Plugin Information

Published: 2007/10/04, Modified: 2020/08/25

Plugin Output

tcp/445/cifs

```
Could not connect to the registry because:
Could not connect to \winreg
```

11011 - Microsoft Windows SMB Service Detection

Synopsis

A file / print sharing service is listening on the remote host.

Description

The remote service understands the CIFS (Common Internet File System) or Server Message Block (SMB) protocol, used to provide shared access to files, printers, etc between nodes on a network.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2002/06/05, Modified: 2020/08/20

Plugin Output

tcp/139/smb

```
An SMB server is running on this port.
```

11011 - Microsoft Windows SMB Service Detection

Synopsis

A file / print sharing service is listening on the remote host.

Description

The remote service understands the CIFS (Common Internet File System) or Server Message Block (SMB) protocol, used to provide shared access to files, printers, etc between nodes on a network.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2002/06/05, Modified: 2020/08/20

Plugin Output

tcp/445/cifs

```
A CIFS server is running on this port.
```

100871 - Microsoft Windows SMB Versions Supported (remote check)

Synopsis

It was possible to obtain information about the version of SMB running on the remote host.

Description

Nessus was able to obtain the version of SMB running on the remote host by sending an authentication request to port 139 or 445.

Note that this plugin is a remote check and does not work on agents.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2017/06/19, Modified: 2019/11/22

Plugin Output

tcp/445/cifs

```
The remote host supports the following versions of SMB :
  SMBv1
  SMBv2
```

106716 - Microsoft Windows SMB2 and SMB3 Dialects Supported (remote check)

Synopsis

It was possible to obtain information about the dialects of SMB2 and SMB3 available on the remote host.

Description

Nessus was able to obtain the set of SMB2 and SMB3 dialects running on the remote host by sending an authentication request to port 139 or 445.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2018/02/09, Modified: 2020/03/11

Plugin Output

tcp/445/cifs

```
The remote host supports the following SMB dialects :
_version_  _introduced in windows version_
2.0.2      Windows 2008
2.1        Windows 7

The remote host does NOT support the following SMB dialects :
_version_  _introduced in windows version_
2.2.2      Windows 8 Beta
2.2.4      Windows 8 Beta
3.0        Windows 8
3.0.2      Windows 8.1
3.1        Windows 10
3.1.1      Windows 10
```

11219 - Nessus SYN scanner

Synopsis

It is possible to determine which TCP ports are open.

Description

This plugin is a SYN 'half-open' port scanner. It shall be reasonably quick even against a firewalled target.

Note that SYN scans are less intrusive than TCP (full connect) scans against broken services, but they might cause problems for less robust firewalls and also leave unclosed connections on the remote target, if the network is loaded.

Solution

Protect your target with an IP filter.

Risk Factor

None

Plugin Information

Published: 2009/02/04, Modified: 2020/08/20

Plugin Output

tcp/135/epmap

```
Port 135/tcp was found to be open
```

11219 - Nessus SYN scanner

Synopsis

It is possible to determine which TCP ports are open.

Description

This plugin is a SYN 'half-open' port scanner. It shall be reasonably quick even against a firewalled target.

Note that SYN scans are less intrusive than TCP (full connect) scans against broken services, but they might cause problems for less robust firewalls and also leave unclosed connections on the remote target, if the network is loaded.

Solution

Protect your target with an IP filter.

Risk Factor

None

Plugin Information

Published: 2009/02/04, Modified: 2020/08/20

Plugin Output

tcp/139/smb

```
Port 139/tcp was found to be open
```

11219 - Nessus SYN scanner

Synopsis

It is possible to determine which TCP ports are open.

Description

This plugin is a SYN 'half-open' port scanner. It shall be reasonably quick even against a firewalled target.

Note that SYN scans are less intrusive than TCP (full connect) scans against broken services, but they might cause problems for less robust firewalls and also leave unclosed connections on the remote target, if the network is loaded.

Solution

Protect your target with an IP filter.

Risk Factor

None

Plugin Information

Published: 2009/02/04, Modified: 2020/08/20

Plugin Output

tcp/445/cifs

```
Port 445/tcp was found to be open
```

11219 - Nessus SYN scanner

Synopsis

It is possible to determine which TCP ports are open.

Description

This plugin is a SYN 'half-open' port scanner. It shall be reasonably quick even against a firewalled target.

Note that SYN scans are less intrusive than TCP (full connect) scans against broken services, but they might cause problems for less robust firewalls and also leave unclosed connections on the remote target, if the network is loaded.

Solution

Protect your target with an IP filter.

Risk Factor

None

Plugin Information

Published: 2009/02/04, Modified: 2020/08/20

Plugin Output

tcp/554

```
Port 554/tcp was found to be open
```

11219 - Nessus SYN scanner

Synopsis

It is possible to determine which TCP ports are open.

Description

This plugin is a SYN 'half-open' port scanner. It shall be reasonably quick even against a firewalled target.

Note that SYN scans are less intrusive than TCP (full connect) scans against broken services, but they might cause problems for less robust firewalls and also leave unclosed connections on the remote target, if the network is loaded.

Solution

Protect your target with an IP filter.

Risk Factor

None

Plugin Information

Published: 2009/02/04, Modified: 2020/08/20

Plugin Output

tcp/2869/www

```
Port 2869/tcp was found to be open
```

19506 - Nessus Scan Information

Synopsis

This plugin displays information about the Nessus scan.

Description

This plugin displays, for each tested host, information about the scan itself :

- The version of the plugin set.
- The type of scanner (Nessus or Nessus Home).
- The version of the Nessus Engine.
- The port scanner(s) used.
- The port range scanned.
- Whether credentialed or third-party patch management checks are possible.
- Whether the display of superseded patches is enabled
- The date of the scan.
- The duration of the scan.
- The number of hosts scanned in parallel.
- The number of checks done in parallel.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2005/08/26, Modified: 2020/08/27

Plugin Output

tcp/0

```
Information about this scan :

Nessus version : 8.11.1
Plugin feed version : 202009081438
Scanner edition used : Nessus Home
Scan type : Normal
Scan policy used : Basic Network Scan
Scanner IP : 192.168.230.128
Port scanner(s) : nessus_syn_scanner
Port range : default
Thorough tests : no
Experimental tests : no
```

```
Paranoia level : 1
Report verbosity : 1
Safe checks : yes
Optimize the test : yes
Credentialed checks : no
Patch management checks : None
Display superseded patches : yes (supersedence plugin launched)
CGI scanning : disabled
Web application tests : disabled
Max hosts : 30
Max checks : 4
Recv timeout : 5
Backports : None
Allow post-scan editing: Yes
Scan Start Date : 2020/9/8 13:25 EDT
Scan duration : 558 sec
```

24786 - Nessus Windows Scan Not Performed with Admin Privileges

Synopsis

The Nessus scan of this host may be incomplete due to insufficient privileges provided.

Description

The Nessus scanner testing the remote host has been given SMB credentials to log into the remote host, however these credentials do not have administrative privileges.

Typically, when Nessus performs a patch audit, it logs into the remote host and reads the version of the DLLs on the remote host to determine if a given patch has been applied or not. This is the method Microsoft recommends to determine if a patch has been applied.

If your Nessus scanner does not have administrative privileges when doing a scan, then Nessus has to fall back to perform a patch audit through the registry which may lead to false positives (especially when using third-party patch auditing tools) or to false negatives (not all patches can be detected through the registry).

Solution

Reconfigure your scanner to use credentials with administrative privileges.

Risk Factor

None

References

XREF IAVB:0001-B-505

Plugin Information

Published: 2007/03/12, Modified: 2020/08/25

Plugin Output

tcp/0

```
It was not possible to connect to '\\WIN-IEJFU67798L\ADMIN$' with the supplied credentials.
```

110723 - No Credentials Provided

Synopsis

Nessus was able to find common ports used for local checks, however, no credentials were provided in the scan policy.

Description

Nessus was unable to execute credentialed checks because no credentials were provided.

Solution

n/a

Risk Factor

None

References

XREF IAVB:0001-B-504

Plugin Information

Published: 2018/06/27, Modified: 2020/08/25

Plugin Output

tcp/0

```
SMB was detected on port 445 but no credentials were provided.
SMB local checks were not enabled.
```

11936 - OS Identification

Synopsis

It is possible to guess the remote operating system.

Description

Using a combination of remote probes (e.g., TCP/IP, SMB, HTTP, NTP, SNMP, etc.), it is possible to guess the name of the remote operating system in use. It is also possible sometimes to guess the version of the operating system.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2003/12/09, Modified: 2020/03/09

Plugin Output

tcp/0

```
Remote operating system : Microsoft Windows 7 Enterprise
Confidence level : 99
Method : MSRPC

Not all fingerprints could give a match. If you think some or all of
the following could be used to identify the host's operating system,
please email them to os-signatures@nessus.org. Be sure to include a
brief description of the host itself, such as the actual operating
system or product / model names.

SinFP:!:
   P1:B11113:F0x12:W8192:O0204ffff:M1460:
   P2:B11113:F0x12:W8192:O0204ffff010303080402080affffffff44454144:M1460:
   P3:B00000:F0x00:W0:O0:M0
   P4:181101_7_p=139


The remote host is running Microsoft Windows 7 Enterprise
```

96982 - Server Message Block (SMB) Protocol Version 1 Enabled (uncredentialed check)

Synopsis

The remote Windows host supports the SMBv1 protocol.

Description

The remote Windows host supports Server Message Block Protocol version 1 (SMBv1). Microsoft recommends that users discontinue the use of SMBv1 due to the lack of security features that were included in later SMB versions. Additionally, the Shadow Brokers group reportedly has an exploit that affects SMB; however, it is unknown if the exploit affects SMBv1 or another version. In response to this, US-CERT recommends that users disable SMBv1 per SMB best practices to mitigate these potential issues.

See Also

https://blogs.technet.microsoft.com/filecab/2016/09/16/stop-using-smb1/

https://support.microsoft.com/en-us/help/2696547/how-to-detect-enable-and-disable-smbv1-smbv2-and-smbv3-in-windows-and

http://www.nessus.org/u?8dcab5e4

http://www.nessus.org/u?234f8ef8

http://www.nessus.org/u?4c7e0cf3

Solution

Disable SMBv1 according to the vendor instructions in Microsoft KB2696547. Additionally, block SMB directly by blocking TCP port 445 on all network boundary devices. For SMB over the NetBIOS API, block TCP ports 137 / 139 and UDP ports 137 / 138 on all network boundary devices.

Risk Factor

None

References

XREF IAVT:0001-T-710

Plugin Information

Published: 2017/02/03, Modified: 2020/08/25

Plugin Output

tcp/445/cifs

```
The remote host supports SMBv1.
```

11153 - Service Detection (HELP Request)

Synopsis

The remote service could be identified.

Description

It was possible to identify the remote service by its banner or by looking at the error message it sends when it receives a 'HELP'

request.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2002/11/18, Modified: 2018/11/26

Plugin Output

tcp/2869/www

```
A web server seems to be running on this port.
```

25220 - TCP/IP Timestamps Supported

Synopsis

The remote service implements TCP timestamps.

Description

The remote host implements TCP timestamps, as defined by RFC1323. A side effect of this feature is that the uptime of the remote host can sometimes be computed.

See Also

http://www.ietf.org/rfc/rfc1323.txt

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2007/05/16, Modified: 2019/03/06

Plugin Output

tcp/0

10287 - Traceroute Information

Synopsis

It was possible to obtain traceroute information.

Description

Makes a traceroute to the remote host.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 1999/11/27, Modified: 2020/08/20

Plugin Output

udp/0

```
For your information, here is the traceroute from 192.168.230.128 to 192.168.230.130 :
192.168.230.128
192.168.230.130

Hop Count: 1
```

35711 - Universal Plug and Play (UPnP) Protocol Detection

Synopsis

The remote device supports UPnP.

Description

The remote device answered an SSDP M-SEARCH request. Therefore, it supports 'Universal Plug and Play' (UPnP). This protocol provides automatic configuration and device discovery. It is primarily intended for home networks. An attacker could potentially leverage this to discover your network architecture.

See Also

https://en.wikipedia.org/wiki/Universal_Plug_and_Play

https://en.wikipedia.org/wiki/Simple_Service_Discovery_Protocol

http://quimby.gnus.org/internet-drafts/draft-cai-ssdp-v1-03.txt

Solution

Filter access to this port if desired.

Risk Factor

None

Plugin Information

Published: 2009/02/19, Modified: 2018/09/12

Plugin Output

udp/1900/ssdp

```
The device responded to an SSDP M-SEARCH request with the following locations :

    http://192.168.230.130:2869/upnphost/udhisapi.dll?content=uuid:a25bbfa2-0f1b-4c02-
af16-4e846fdf35aa

And advertises these unique service names :

    uuid:a25bbfa2-0f1b-4c02-af16-4e846fdf35aa::urn:schemas-upnp-org:service:ConnectionManager:1
    uuid:a25bbfa2-0f1b-4c02-
af16-4e846fdf35aa::urn:microsoft.com:service:X_MS_MediaReceiverRegistrar:1
    uuid:a25bbfa2-0f1b-4c02-af16-4e846fdf35aa::urn:schemas-upnp-org:service:ContentDirectory:1
    uuid:a25bbfa2-0f1b-4c02-af16-4e846fdf35aa::upnp:rootdevice
    uuid:a25bbfa2-0f1b-4c02-af16-4e846fdf35aa::urn:schemas-upnp-org:device:MediaServer:1
    [fe80::b8be:1ed5:70b0:a381]:3540
```

20094 - VMware Virtual Machine Detection

Synopsis

The remote host is a VMware virtual machine.

Description

According to the MAC address of its network adapter, the remote host is a VMware virtual machine.

Solution

Since it is physically accessible through the network, ensure that its configuration matches your organization's security policy.

Risk Factor

None

Plugin Information

Published: 2005/10/27, Modified: 2019/12/11

Plugin Output

tcp/0

```
The remote host is a VMware virtual machine.
```

135860 - WMI Not Available

Synopsis

WMI queries could not be made against the remote host.

Description

WMI (Windows Management Instrumentation) is not available on the remote host over DCOM. WMI queries are used to gather information about the remote host, such as its current state, network interface configuration, etc.

Without this information Nessus may not be able to identify installed software or security vunerabilities that exist on the remote host.

See Also

https://docs.microsoft.com/en-us/windows/win32/wmisdk/wmi-start-page

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2020/04/21, Modified: 2020/08/31

Plugin Output

tcp/445/cifs

```
Can't connect to the 'root\CIMV2' WMI namespace.
```

35712 - Web Server UPnP Detection

Synopsis

The remote web server provides UPnP information.

Description

Nessus was able to extract some information about the UPnP-enabled device by querying this web server. Services may also be reachable through SOAP requests.

See Also

https://en.wikipedia.org/wiki/Universal_Plug_and_Play

Solution

Filter incoming traffic to this port if desired.

Risk Factor

None

Plugin Information

Published: 2009/02/19, Modified: 2020/06/12

Plugin Output

tcp/2869/www

```
Here is a summary of http://192.168.230.130:2869/upnphost/udhisapi.dll?
content=uuid:a25bbfa2-0f1b-4c02-af16-4e846fdf35aa :

deviceType: urn:schemas-upnp-org:device:MediaServer:1
friendlyName: WIN-IEJFU67798L: Admin:
manufacturer: Microsoft Corporation
manufacturerURL: http://www.microsoft.com
modelName: Windows Media Player Sharing
modelName: Windows Media Player Sharing
modelNumber: 12.0
modelURL: http://go.microsoft.com/fwlink/?LinkId=105926
serialNumber: {1F460276-B34D-401F-99FC-D22430E8CFF1}
ServiceID: urn:upnp-org:serviceId:ConnectionManager
serviceType: urn:schemas-upnp-org:service:ConnectionManager:1
controlURL: /upnphost/udhisapi.dll?control=uuid:a25bbfa2-0f1b-4c02-af16-4e846fdf35aa+urn:upnp-
org:serviceId:ConnectionManager
eventSubURL: /upnphost/udhisapi.dll?event=uuid:a25bbfa2-0f1b-4c02-af16-4e846fdf35aa+urn:upnp-
org:serviceId:ConnectionManager
SCPDURL: /upnphost/udhisapi.dll?content=uuid:8816b825-9a12-45d7-bda5-c6ca047c8cc8
ServiceID: urn:upnp-org:serviceId:ContentDirectory
serviceType: urn:schemas-upnp-org:service:ContentDirectory:1
controlURL: /upnphost/udhisapi.dll?control=uuid:a25bbfa2-0f1b-4c02-af16-4e846fdf35aa+urn:upnp-
org:serviceId:ContentDirectory
```

```
eventSubURL: /upnphost/udhisapi.dll?event=uuid:a25bbfa2-0f1b-4c02-af16-4e846fdf35aa+urn:upnp-
org:serviceId:ContentDirectory
SCPDURL: /upnphost/udhisapi.dll?content=uuid:c2afcf8c-4a34-41cd-be74-7b5177430ba5
ServiceID: urn:microsoft.com:serviceId:X_MS_MediaReceiverRegistrar
serviceType: urn:microsoft.com:service:X_MS_MediaReceiverRegistrar:1
controlURL: /upnphost/udhisapi.dll?control=uuid:a25bbfa2-0f1b-4c02-af16-4e846fdf35aa
+urn:microsoft.com:serviceId:X_MS_MediaReceiverRegistrar
eventSubURL: /upnphost/udhisapi.dll?event=uuid:a25bbfa2-0f1b-4c02-af16-4e846fdf35aa
+urn:microsoft.com:serviceId:X_MS_MediaReceiverRegistrar
SCPDURL: /upnphost/udhisapi.dll?content=uuid:d8fc306d-c9a7-4669-a4dd-fd002ecd334b
```

10150 - Windows NetBIOS / SMB Remote Host Information Disclosure

Synopsis

It was possible to obtain the network name of the remote host.

Description

The remote host is listening on UDP port 137 or TCP port 445, and replies to NetBIOS nbtscan or SMB requests.

Note that this plugin gathers information to be used in other plugins, but does not itself generate a report.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 1999/10/12, Modified: 2020/08/20

Plugin Output

udp/137/netbios-ns

```
The following 6 NetBIOS names have been gathered :

 WIN-IEJFU67798L  = Computer name
 WORKGROUP        = Workgroup / Domain name
 WIN-IEJFU67798L  = File Server Service
 WORKGROUP        = Browser Service Elections
 WORKGROUP        = Master Browser
 __MSBROWSE__     = Master Browser

The remote host has the following MAC address on its adapter :

   00:0c:29:d9:0d:13
```